**Biometric Payments: Overview**

****

## **Leveraging biology to elevate payment technology**

### Biometric payments are evolving authentication from something users own and know (such as PINs/passwords and payment cards/smartphones) to simply who they are.

### Biometrics refers to the use of biological measurements and physical characteristics to identify an individual for situations including identity verification, user authentication, and access controls. These technologies are also increasingly being adopted to verify payments, ensuring a secure and convenient method for authorizing payments in person and online.

### These emerging biometric payment technologies can broadly be defined as any hardware or software that enables point-of-sale (POS) authentication using unique physical or biological markers to identify users and authorize payments and other financial transactions.

### 

### 

### 

### 

### 

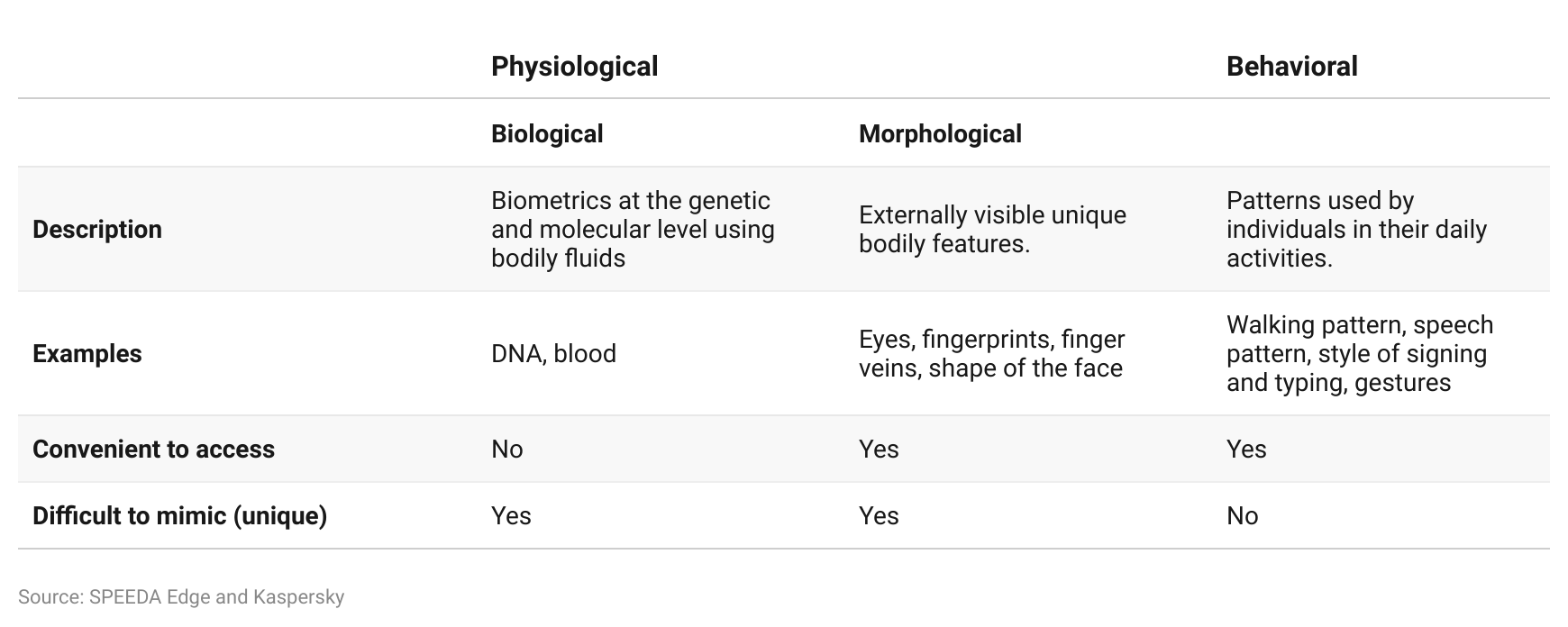
### **Biometric data replaces PINS and Passwords**

****

Source: SPEEDA Edge

Biometrics are broadly classified as biological, morphological, and behavioral with payment authentication methods primarily relying on morphological features.

### **Morphological biometrics win on convenience and security**



### Factors such as accuracy, size of template, contactless nature, long-term stability, and cost play a key role in deciding which type of morphological biometric is used to authenticate payments. Deciding whether it is fit for the purpose typically depends on reaching a balance between cost and accuracy. Therefore, using one’s fingerprint, finger vein, and facial recognition remain the most common ways of authenticating payments.

### **Facial recognition, fingerprint, and finger veins strike balance between cost and accuracy**

****

*Note: FAR is the false acceptance rate and FRR denotes the false rejection rate; although the use of voice tech and iris and retina identification for payment is less common, they still exist.*

Source: SPEEDA Edge research

Regardless of the types of biometric used, biometric payments can be made in three main ways: in-store through terminals, payment cards, and mobile payment applications. This report excludes automated stores and companies enabling users to shop and pay with their smart speakers through voice recognition.

### 

### 

### 

### 

### 

### 

### **The market can be segmented based on end-use**

A screenshot of a white sheet

Description automatically generated

## **High accuracy and falling cost of embedding sensors is a key industry enabler**

### To use biometrics as a form of authenticating payments, biometric sensors must be able to identify people accurately, at least as accurately as traditional forms of payment authentication (such as PINs or signatures). The accuracy of biometric sensors typically relies on two factors: 1) false acceptance rate (FAR) and 2) false rejection rate (FRR), both of which are at relatively low levels for biometric authentication, in general, despite varying by type.

### In addition to accuracy, the cost of biometrics systems has also played a key role in enabling its use. High cost of sensors could hamper merchant and issuer uptake of biometric payment authentication, given the existence of low-cost POS terminals in the market. Using the cost of mobile fingerprint sensors as a proxy for the broader biometric sensors market, Carnegie Research estimates that the average selling price (ASP) of fingerprint sensors globally has more than halved to USD 2.10 in 2019 (from USD 5.50 in 2014).

### In addition to these, integrating biometrics into smart devices and payment cards has had a positive impact as follows:

### **Impact of embedding biometrics to smart devices and payment cards**



# **Driving Factors**

**1. Mitigating card fraud by improving transaction security**

SmartMetric estimates that around 80% of all credit cards in circulation have been impacted by a hack or data breach (as of March 2024). Meanwhile, card fraud losses amounted to USD 34 billion globally in 2022, with the US accounting for 34%. Studies have indicated that nearly 30% of card fraud losses are attributed to the misuse of payment cards that are lost or stolen, and a further 16% are attributed to counterfeit card fraud. Biometric payment cards should help mitigate these losses by addressing phishing, accidental data leaks, and shoulder surfing; however, other forms of fraud such as application fraud and account takeovers may not be fully addressed by these cards, as bad actors could hack directly into data sources to breach data.

### However, although biometric payment forms are susceptible to the risk of hacking, biometric payment cards reduce this risk by decentralizing the biometric data by retaining and processing of the biometric data on the cards itself, rather than on third-party systems, such as with banks, retailers, or payment apps. Moreover, two-factor authentications have also been adopted by biometric payment card solution providers to improve safety.

### Adopting biometric payments to mitigate security concerns is supported by users perceiving biometrics as the most secure form of authentication currently available. Studies have indicated that a majority of respondents feel biometrics are more secure than legacy authentication methods for log-ins. It is likely this same sentiment applies to payment authentication.

**2. Improving user convenience by uplifting contactless card limits**

## While offering users enhanced security benefits all segments, the contactless card segment particularly benefits, as tighter security means paving the way to raise transaction limits. These limits have been a key constraint to contactless card adoption, as around 79% of banks, surveyed across the globe in 2020, believed that payment caps were the main contactless card-related frustration for users.

## Contactless cards have reduced security, as no PINs nor signatures are needed to authenticate transactions; however, they offer high convenience and transaction speeds, and, therefore, remain quite popular (contactless cards were used for ~85% of grocery transactions in the US as of November 2023). It is notable that ~51% of Americans reportedly used contactless payment methods (November 2023; including mobile wallets and contactless payment cards), and studies indicated that more than 90% of debit cards issued in the US in 2023 were expected to be contactless cards. Therefore, biometric payment cards are likely to play a crucial role in balancing the convenience offered by contactless cards, with the necessary security, to drive further adoption.

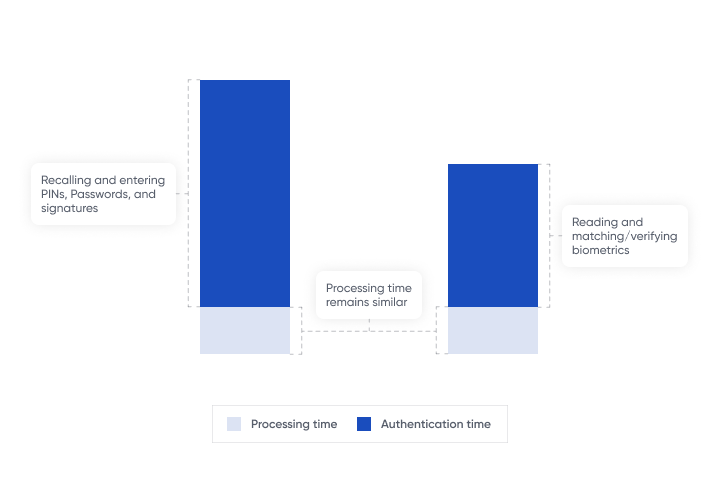
**3. Increasing customer convenience through faster checkouts**

Biometrics offers more convenient and faster checkouts at brick-and-mortar stores. Users can avoid the hassle and effort of entering PINs/signatures, while users of in-store biometrics benefit more from not having to sift through their cards and mobile phones to complete payments. Moreover, biometrics also avoid common pitfalls of traditional payments, such as damaged credit cards, losing or forgetting the smartphone/payment cards, the phone/device dying, or losing/forgetting the PIN/password.

### Passwords can be challenging to remember, as there has been an increase in the average number of passwords used by an individual (~100 per person in 2020 from 70–80 per person in 2019). As a result, security can be compromised, as one in three Americans prefer to have an easier to remember password than a secure one. Moreover, studies have indicated that ~11% of respondents use the same password across all their accounts.

### In-store biometric payment terminals and biometric payment cards also save time by reducing transaction time, including processing and authentication, to around one second total. Traditional payment cards, in contrast, take more time as they require users to sign and/or recall and enter PINs for authentication.

### **Biometrics reduces the overall transaction time**

****

*Note: Please note the proportions in the above diagram are purely for illustrations and not a representation of the exact relative transaction times.*

Source: SPEEDA Edge

## 

**4. Enhances ROI for card issuers and merchants by offering additional revenue streams at low incremental cost**

### Entities issuing credit cards (primarily banks and other financial institutions) can gain ROI by shifting to biometric payments cards, mainly by charging its users an issuing fee (credit cards typically do not have issuing fees and instead only charge annual fees and interest).

### A study on credit card users in the US indicated that about 70% of respondents were willing to pay an upfront charge of USD 70 for biometric security in credit cards. Moreover, around 57% of respondents across the globe in 2022 indicated they would even consider switching banks to one that offers biometric payment cards.

### ABI Research estimates that the cost of producing a biometric payment card as of early-2021 is USD 20–30 and believes that it should fall to around USD 10 by 2025/26 and USD 5 by 2027/28 as volumes increase. Volume is likely to play a substantial role in reducing the cost, given that the cards use standard versions of payment card components - such as security elements (SEs) - and standard manufacturing processes, with the main incremental addition being the biometric sensors, which can cost around USD 3 per card (as of 2020).

### Moreover, credit card issuers may gain more from cost savings by eliminating the administrative activities relating to issuing PINs for the cards, such as posting out PINs and verifying identities of new customers.

### Besides the card issuers, merchants are likely to see enhanced returns through the higher use of biometric cards, as they should lead to higher spending as contactless card transaction limits are raised. Moreover, the higher return comes with no incremental cost—the merchants do not need to upgrade their payment terminals, as biometric cards are compatible with existing ones.

# **Risks**

## **1. Biometric data can be hacked**

## Although authentication information cannot be leaked to unauthorized parties, biometrics can still be susceptible to hacking. The stolen data can be used for payment authentication fraudulently, and such a data compromise is likely to be more harmful with biometrics than PINs and passwords, as the latter can be changed. Payment companies managing biometric data could be vulnerable to hacking, as even large US government agencies have been hacked. For instance, the Office of Personnel Management was hacked in 2015, and 5.6 million fingerprint IDs were stolen. More recently, biometric data of more than a million people across several countries, including the US, the UK, India, and Japan, were compromised in a data breach in 2019.

## Such attacks can cost payment technology providers in several ways, including liability for stolen assets or information, costs of repairing damage to internal systems, and lost income resulting from system downtime owing to such breaches.

## In addition to costing businesses in the case of data breaches, fearing such breaches might lead users to avoid using biometric payments altogether (a study in 2020 noted that around 69% of respondents were concerned about data breaches).

## Companies have turned to innovation to reduce their exposure to the risk of hacking. For instance, in-store and remote biometric payment tech provider TouchToPay claims its system is enhanced against security threats, as it uses mathematical algorithms corresponding to users’ fingerprints and does not store the full image of user fingerprints.

**2. Lengthy development cycles increase payback risk for biometric card technology providers**

## Developing biometric payment card sensors and technology that is market-ready can be a resource-heavy and time-intensive process. Beyond being able to recognize and authenticate biometrics, the sensors should also be able to distinguish between live and fake fingerprints (anti-spoofing technology) to be fully prepared for commercial use and be certified by leading payment networks. Despite leading disruptors such as IDEX Biometrics and SmartMetric having been in the industry for over two decades, it is due to these challenges that they largely began commercializing their products in 2022. Even after commercializing their biometric card tech, companies may struggle to recover their investments. For instance, IDEX Biometrics’ (IDEX’s) accumulated losses as of 2023 were nearly 80x its revenue in 2023.

## Meanwhile, Zwipe, an inlay provider for access control cards and biometric payment cards, decided to exit the biometric payment card market in January 2024 – despite being certified by Visa and Mastercard and spending decades in the market – as it felt market adoption and commercial launches fell short of its expectations.

**3. Tightening regulations relating to privacy and handling biometric data**

Biometric data is personal, and is, therefore, regulated by a range of laws relating to both biometrics and privacy. In the US, although there is no common federal law governing biometrics and privacy, the Gramm-Leach-Bliley Act of 1999 impacts financial institutions in their dealing with personally identifiable financial information, which can include biometrics data used to verify payments.

## In terms of laws specific to biometrics, some states have chosen to regulate the collection, use, and retention of biometric data. The Illinois Biometric Payment Act (BIPA) enacted in 2008 was the first and strictest biometric payment law in the US and acted as the model for laws developed in other states, including Texas (2009) and Washington (2017).

## In addition to laws governing biometrics usage, privacy laws have continued to tighten. The California Consumer Protection Act (CCPA; took effect in January 2020) is the main privacy law in the US, and it offers several rights to consumers relating to their personal biometric data, such as the right to access, delete, move the data, and opt out of programs. Moreover, privacy laws are likely to continue tightening in the US, as other states follow California’s lead, such as the Virginia Consumer Data Protection Act (CDPA) and the Colorado Privacy Act (CPA), which took effect in 2023.

## Biometric payment companies failing to comply with the above (and other such) laws, much like any other FinTechs, can be penalized for misusing personal data. For instance, in February 2023, Veriff, an identity verification infrastructure provider, agreed to pay USD 4 million to settle a class action lawsuit filed against it under the BIPA, for allegedly failing to comply with BIPA, in relation to obtaining consent before collecting facial geometry scans for identity verification.

**4. Concentrated end market for biometric payment card tech**

Biometric payment card tech providers primarily offer their technology to card manufacturers, which is a relatively concentrated end market, as IDEX noted that the six largest companies accounted for around 70% of the revenue generated from the shipment of smart cards for financial payments in 2022. Concentration in the end market may lead to the revenue of key disruptors being dependent on a few end customers. For instance, IDEX’s two largest customers accounted for more than 67%–73% of its revenue over 2022–2023.

*Last updated: June 2024*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.